مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Cisco Security Updates

Tracking #:432316357

Date:03-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Cisco has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Cisco has released security updates to address multiple vulnerabilities in various products, including Nexus Dashboard, Small Business Routers, Meraki Teleworker Gateways, and others. These vulnerabilities could potentially allow attackers to execute remote code, escalate privileges, cause denial of service, or disclose sensitive information on affected systems.

Vulnerabilities Details:

Description	CVE	Severity
Cisco Nexus Dashboard Fabric Controller Arbitrary Command Execution Vulnerability	CVE-2024-20432	Critical
Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers Privilege Escalation and Remote Command Execution Vulnerabilities	CVE-2024-20393 CVE-2024-20470	High
Cisco Nexus Dashboard Fabric Controller Remote Code Execution Vulnerability	CVE-2024-20449	High
Cisco Meraki MX and Z Series Teleworker Gateway AnyConnect VPN Denial of Service Vulnerabilities	CVE-2024-20498 CVE-2024-20499 CVE-2024-20500	High
Cisco Small Business RV042, RV042G, RV320, and RV325 Routers Denial of Service and Remote Code Execution Vulnerabilities	CVE-2024-20516 CVE-2024-20517 CVE-2024-20518	Medium
Cisco Nexus Dashboard Orchestrator SSL/TLS Certificate Validation Vulnerability	CVE-2024-20385	Medium
Cisco Nexus Dashboard and Nexus Dashboard Fabric Controller Unauthorized REST API Vulnerabilities	CVE-2024-20438 CVE-2024-20441 CVE-2024-20442	Medium
Cisco Nexus Dashboard Hosted Services Information Disclosure Vulnerabilities	CVE-2024-20490 CVE-2024-20491	Medium
Cisco Nexus Dashboard Fabric Controller REST API Command Injection Vulnerability	CVE-2024-20444	Medium
Cisco Nexus Dashboard Fabric Controller Configuration Backup Information Disclosure Vulnerability	CVE-2024-20448	Medium
Cisco Meraki MX and Z Series Teleworker Gateway AnyConnect VPN Session Takeover and Denial of Service Vulnerability	CVE-2024-20509	Medium
Cisco Identity Services Engine Information Disclosure Vulnerability	CVE-2024-20515	Medium
Cisco Expressway Series Privilege Escalation Vulnerability	CVE-2024-20492	Medium
Cisco UCS B-Series, Managed C-Series, and X-Series Servers Redfish API Command Injection Vulnerability	CVE-2024-20365	Medium
Cisco Catalyst 9000 Series Switches Denial of Service Vulnerability	CVE-2024-20434	Medium

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Cisco.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://sec.cloudapps.cisco.com/security/center/publicationListing.x